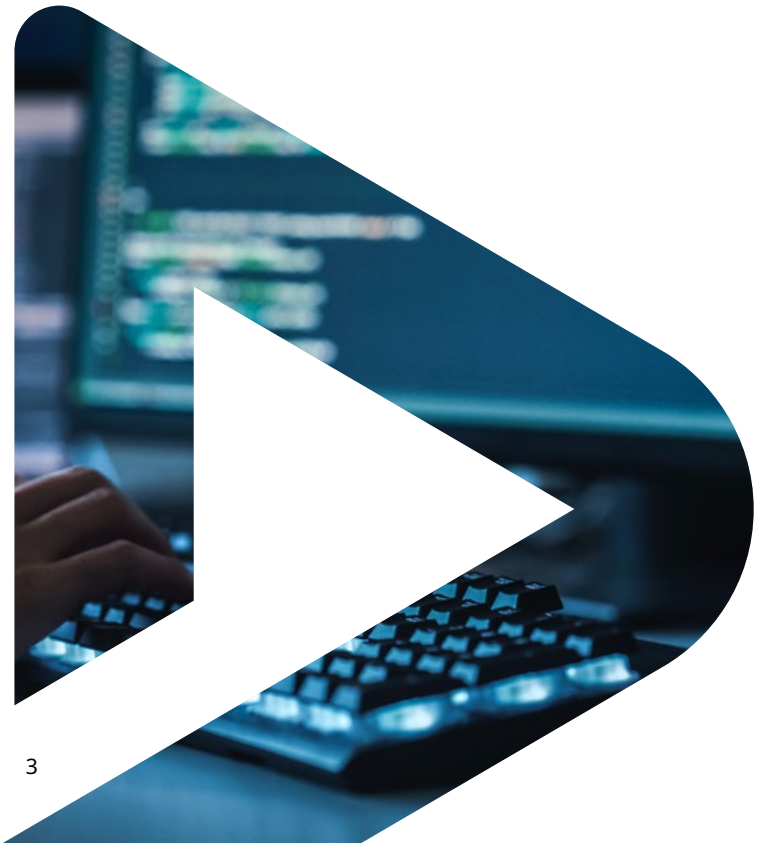
ISO/IEC 27001

Strateginen työkalu tietoturvallisuuden **hallintaan ja johtamiseen**

Sisältö

01 Mikä on ISO/IEC 27001 **-tietoturvallisuuden hallintajärjestelmä?**

ISO/IEC 27001 on kansainvälisesti tunnustettu standardi, joka auttaa organisaatioita järjestelmällisesti suojaamaan tietojaan ja hallitsemaan tietoturvariskejä. Standardi määrittelee vaatimukset tietoturvallisuuden hallintajärjestelmälle (Information Security Management System, ISMS), jonka avulla organisaatio pystyy tunnistamaan, arvioimaan ja hallitsemaan tietoturvariskejä suunniteltujen prosessien avulla. Standardin ensimmäinen versio julkaistiin vuonna 2005 ja sen takana ovat yhteistyössä kansainväliset standardisoimisjärjestöt ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission).



02 Miksi systemaattinen **tietoturvallisuuden hallinta on tärkeää?**

Tietoturvallisuus tarkoittaa organisaation tietojen, järjestelmien ja datan suojaamista erilaisilta uhkilta, vahingoilta ja väärinkäytöksiltä. Sen keskeisiä tavoitteita ovat tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistaminen. Systemaattinen tietoturvallisuuden hallinta on organisaatioille yhä tärkeämpää, sillä digitalisaatio on lisännyt valtavasti riippuvuutta digitaalisista palveluista ja kasvattanut kyberuhkien määrää.

Uhat	Vaikutukset
Tietomurrot →	Liiketoiminnan keskeytyminen
Palvelunestohyökkäykset →	Taloudelliset menetykset
Haittaohjelmat →	Mainehaitat
Tietovuodot →	Asiakasluottamuksen heikkeneminen
Toimitusketjun riskit →	Sopimus- ja sääntelyriskit

Myös sääntely edellyttää yhä enemmän kyber- ja tietoturvallisuudelta: esimerkiksi kyberturvallisuuslaki (NIS2-direktiivi), tietosuoja (GDPR-direktiivi) ja toimitusketjuihin liittyvät tietoturvavaatimukset edellyttävät organisaatioilta ennakoivaa ja järjestelmällistä tietoturvallisuuden johtamista nopeasti muuttuvassa ja monimutkaistuvassa toimintaympäristössä.

Keskeisiä yrityksien tietoturvauhkia ovat: haittaohjelmat ja kiristysohjelmat, tietojenkalastelu, inhimilliset virheet ja sosiaalinen manipulointi, vanhentuneet järjestelmät ja ohjelmistot sekä toimitusketjun tietoturvariskit.

03 Miten ISO/IEC 27001 auttaa **hallitsemaan tietoturvallisuutta?**

ISO/IEC 27001 tarjoaa organisaatiolle systemaattisen toimintamallin tietoturvallisuuden johtamiseen ja kehittämiseen. Standardin tavoitteena on auttaa organisaatiota tunnistamaan tietoturvariskit, suojaamaan tieto-omaisuuttaan ja varmistamaan liiketoiminnan jatkuvuus muuttuvassa toimintaympäristössä.

Standardin kuvaaman ja vaatiman toimintamallin kova ydin on tietoturvariskien hallinta, joka perustuu kahteen prosessiin: tietoturvariskien arviointi ja tietoturvariskien käsittely. Näiden mukaisesti organisaation tulee tunnistaa, arvioida ja käsitellä tietoturvariskejä suunnitelmallisesti ja vaikuttavasti. Riskienhallinnan kohteena on tieto kaikissa muodoissaan. Digitaalisten järjestelmien lisäksi riskienhallinta kattaa kaikki tietoon sekä tiedon käsittelyyn ja säilytykseen liittyvät elementit, kuten laitteet, tietoverkot, fyysiset tilat, paperi- ja mikrofilmiarkistot, henkilöstön ja toimintaprosessit.

ISO/IEC 27001 auttaa organisaatiota rakentamaan selkeät käytännöt muun muassa:

- tietoturvaperiaatteiden ja -tavoitteiden määrittelyyn
- roolien ja vastuiden hallintaan
- henkilöstön tietoisuuden ja osaamisen kehittämiseen
- riskienhallintaan ja poikkeamien käsittelyyn
- seurannan, auditointien ja jatkuvan parantamisen toteuttamiseen.

04 Mitä hyötyä ISO/IEC 27001 **-sertifioinnista on yritykselle?**

ISO/IEC 27001 -sertifiointi osoittaa asiakkaille, yhteistyökumppaneille ja muille sidosryhmille, että organisaation tietoturvallisuutta johdetaan kansainvälisesti tunnustetun standardin mukaisesti. Sertifiointi tukee riskienhallintaa, liiketoiminnan jatkuvuutta ja organisaation luotettavuutta.

Sertifioidun tietoturvallisuuden hallintajärjestelmän avulla organisaatio voi:

- pienentää tietosuoja-, maine- ja jatkuvuusriskejä
- sujuvoittaa toimintaa ja vähentää kustannuksia
- vahvistaa asiakkaiden ja sidosryhmien luottamusta
- parantaa kilpailukykyä markkinoilla
- vastata esimerkiksi kyberturvallisuuslain (NIS2-direktiivin), tietosuojan (GDPR-direktiivi) sekä asiakkaiden ja toimitusketjujen tietoturvavaatimuksiin.

05 Mille toimialoille **ISO/IEC 27001 sopii?**

ISO/IEC 27001 soveltuu kaikille toimialoille, sillä käytännössä kaikki yritykset käyttävät tietojärjestelmiä ja ovat riippuvaisia niiden toimivuudesta ja tieto-omaisuuden turvaamisesta. ISO/IEC 27001 skaalautuu toimialan ja organisaation koon mukaan, ja sen mukainen sertifiointi on vahva viesti tietojen suojaamiseen sitoutumisesta sekä sisäisesti että ulkoisesti.

06 Onko ISO/IEC 27001 yhteensopiva **muiden standardien kanssa?**

Kyllä. ISO/IEC 27001 on vaatimusosaltaan kompaktina erittäin hyvin yhteensopiva muiden johtamisjärjestelmästandardien kanssa. Standardi voidaan helposti integroida olemassa olevaan johtamisjärjestelmään, mikä mahdollistaa myös yhdistetyt sertifioinnit.

Yhteensopivia standardeja ovat esimerkiksi:

- ISO 9001 (laadunhallinta)
- ISO 14001 (ympäristöjohtaminen)
- ISO 45001 (työterveys ja -turvallisuus)
- ISO 22301 (liiketoiminnan jatkuvuudenhallinta)
- ISO/IEC 20000-1 (palveluidenhallinta)
- ISO/IEC 42001 (tekoälyn hallinta)

Integroimisen etuja:

- tehokkaampi johtamisjärjestelmä
- yhtenäiset prosessit
- vähemmän päällekkäistä dokumentaatiota
- tehokkaammat auditoinnit
- parempi kokonaisriskien hallinta.

07 ISO/IEC 27001 -sertifioinnin **tarkistuslista**

Tarkistuslistamme avulla saat nopeasti ja helposti selville, onko yrityksesi valmis ISO/IEC 27001 -standardin mukaiseen tietoturvallisuuden hallintajärjestelmän sertifiointiin.

Seuraavat kysymykset noudattavat johtamisjärjestelmästandardien perusrakennetta. Jos voit vastata kysymykseen kyllä, merkitse se rastilla. Näin näet nopeasti, mitkä osa-alueet yrityksessäsi täyttävät jo vaatimukset, ja mitkä osa-alueet vaativat vielä kehittämistä

TARKISTUSLISTA – ISO/IEC 27001 tietoturvallisuuden hallintajärjestelmä

Organisaation toimintaympäristö

- [ ] Organisaatiolla on näyttö siitä, että tietoturvallisuuteen ja sen hallintaan liittyvät prosessit toteutetaan oikein, niitä ohjataan ja niiden suorituskykyä mitataan.
- [ ] Tietoturvariskien arviointia tehdään suunnitelluin aikavälein ja vähintään merkittävien muutosten yhteydessä.
- [ ] Tietoturvariskejä käsitellään tietoturvallisuuden hallintakeinoja toteuttamalla siten, että ne ovat siedettävällä tasolla.

Johtaminen

- [ ] Tietoturvapolitiikkaa tukevat tavoitteet ja vaatimukset on määritelty ja dokumentoitu.
- [ ] Ylin johto, joka vastaa ISMS:n ohjauksesta ja resurssien käytöstä, on määritelty.
- [ ] Tietoturvallisuuden hallinnolliset ja tekniset erityisroolit vastuineen on määritetty.
- [ ] Tietoturvapolitiikka on otettu käyttöön mm. ylimmän johdon viestimänä.

Suunnittelu

- [ ] Organisaatiossa on dokumentoitu tietoturvariskien arviointiprosessi.
- [ ] Organisaatiossa on dokumentoitu tietoturvariskien käsittelyprosessi.
- [ ] Riskien arvioinnin ja riskien käsittelyn prosesseista on kattava dokumentointi tai suunnitelma.
- [ ] Kaikki riskien arviointien ja analyysien tulokset on tallennettu.
- [ ] Kaikki riskien käsittelyyn liittyvät tiedot ja tulokset on dokumentoitu.
- [ ] On laadittu soveltuvuuslausunto (Statement of Applicability, SoA), joka dokumentoi toteutettavat tietoturvariskien hallintakeinot vähintään standardin liitteestä A, sekä niiden perustelut.
- [ ] Organisaatiolle on määritelty tietoturvatavoitteet.

Tuki

- [ ] Tietoturvallisuuteen liittyvään sisäiseen ja ulkoiseen viestintään on viestintäsuunnitelma tai -matriisi.
- [ ] ISMS:n toteuttamiseen ja hallintaan on tarvittavat resurssit (henkilöstö ja infrastruktuuri) .
- [ ] Dokumentoidun tiedon hallintaan on menettelyt.
- [ ] ISMS:ään liittyvien roolien (esim. CISO) pätevyydet on määritelty ja dokumentoitu.
- [ ] ISMS:n perehdytys-, tietoisuus- ja koulutuskonsepti on luotu.
- [ ] Organisaatiolla on ISMS-koulutusmateriaalit ja näyttö siitä, että henkilöstö on osallistunut asiaankuuluviin koulutuksiin.

Toiminta

- [ ] Organisaatiolla on näyttö siitä, että tietoturvallisuuteen ja sen hallintaan liittyvät prosessit toteutetaan oikein, niitä ohjataan ja niiden suorituskykyä mitataan.
- [ ] Tietoturvariskien arviointia tehdään suunnitelluin aikavälein ja vähintään merkittävien muutosten yhteydessä.
- [ ] Tietoturvariskejä käsitellään tietoturvallisuuden hallintakeinoja toteuttamalla siten, että ne ovat siedettävällä tasolla.

Suorituskyvyn arviointi

- [ ] Tietoturvatavoitteiden kanssa linjassa olevat mittarit ja niiden analysoinnin käytännöt on määritetty.
- [ ] Sisäisen auditoinnin toteutustavat sekä pitkän (3 vuotta) ja lyhyen (vuosi) aikavälin auditointiohjelmat on laadittu.
- [ ] Sisäistä auditointia on tehty ja raportoitu.
- [ ] Ylimmän johdon tekemä katselmus hallintajärjestelmän tilaan on suunniteltu, pidetty ja sen tulokset dokumentoitu.

Jatkuva parantaminen

- [ ] Poikkeamista, korjaavista toimenpiteistä ja niiden tuloksista on näyttöä.

Autamme sinua sertifioimaan onnistuneesti tietoturvallisuuden hallintajärjestelmäsi ISO/IEC 27001 -standardin mukaisesti.

Ota yhteyttä

08 DEKRAn ISO/IEC 27001 -sertifikaatti **seitsemässä vaiheessa**

01

Sertifioinnin valmistelu ja vapaaehtoinen nykytilan arviointi

Keskustelu johtamisjärjestelmän tilasta, standardin vaatimuksista ja sertifiointiprosessista. Tarvittaessa johtamisjärjestelmän nykytilan arviointi syötteeksi vielä tarvittavaan kehittämiseen.

02

Johtamisjärjestelmän sertifiointi

Kaksivaiheinen auditointi johtamisjärjestelmän dokumentointiin ja käytännön toteutukseen. Vaiheessa 1 arvioidaan dokumentoinnin vaatimustenmukaisuus. Vaihe 2 toteutetaan lähtökohtaisesti kohdeorganisaation tiloissa ja se sisältää dokumentoinnin tarkempaa läpikäyntiä ja haastatteluita.

03

Auditointiraportti ja korjaavat toimenpiteet

Johtamisjärjestelmän auditoinnin tulosten dokumentointi. Tarvittaessa tehdään jälkiarviointi poikkeamien korjaavien toimenpiteiden arvioimiseksi.

04

Sertifikaatti ja sinetti

Vaatimusten täyttyessä myönnetään sertifikaatti ja DEKRA-sinetti. Sertifikaatti on voimassa kolme vuotta.

05

Ensimmäinen seuranta-auditointi

Sertifikaatin myöntöpäivästä 12 kk kuluessa tehtävä, sertifiointia selvästi pienempi auditointi raportointeineen. Keskeinen teema on jatkuvan parantamisen ja kehittymisen arviointi.

06

Toinen seuranta-auditointi

Sertifikaatin myöntöpäivästä 24 kk kuluessa tehtävä, sertifiointia selvästi pienempi auditointi raportointeineen. Keskeinen teema on jatkuvan parantamisen ja kehittymisen arviointi.

07

Uudelleensertifiointi

Joitakin kuukausia ennen sertifikaatin voimassaolon päättymistä tehtävä, jatkuvan vaatimustenmukaisuuden toteutumisen varmistava auditointi. Vaatimusten täyttyessä myönnetään uusi sertifikaatti kolmeksi vuodeksi ja toistetaan kohdat 5 - 7.

09 Mikä on ISO/IEC 27001 **-standardin merkitys ja vaikutus?**

ISO/IEC 27001 -standardin tavoitteena on auttaa organisaatioita hallitsemaan tietoturvallisuutta järjestelmällisesti, jatkuvasti ja vaikuttavasti. Standardi tuo rakenteen tietoturvariskien hallintaan sekä tukee liiketoiminnan jatkuvuutta nopeasti muuttuvassa digitaalisessa toimintaympäristössä.

Tietoturvallisuus ei ole vain tekninen kysymys, vaan keskeinen osa organisaation johtamista, riskienhallintaa ja luotettavuutta. ISO/IEC 27001 auttaa organisaatioita rakentamaan yhtenäisen toimintamallin, jossa tietoturvallisuus integroidaan osaksi päivittäisiä prosesseja ja päätöksentekoa.

Standardin keskeinen vaikutus syntyy siitä, että tietoturvallisuutta kehitetään jatkuvasti osana organisaation johtamisjärjestelmää. Tämä auttaa organisaatiota varautumaan muutoksiin, kehittämään toimintaa pitkäjänteisesti ja vastaamaan sekä asiakkaiden että viranomaisten kasvaviin odotuksiin ja vaatimuksiin.

Mitä DEKRA tarjoaa?

DEKRAn ISO/IEC 27001 -auditoinneissa kokeneet asiantuntijamme suunnittelevat tarkasti auditointien sisällön ja kohteet yhteistyössä kanssanne. Auditoijiemme osaaminen on laaja-alaista, jolloin pystymme tuomaan teille lisäarvoa vaativan standardin auditoinnissa. Tärkein tehtävämme on arvioida standardin vaatimusten täyttyminen, mutta sen ohessa autamme asiakkaitamme kehittymään standardiin kirjatuista vaatimuksista pidemmälle.

Kansainvälisesti tunnustettu DEKRA-sertifiointi ja DEKRA-sinetti osoittavat organisaation sitoutumisen tietoturvallisuuden hallintaan ja vahvistavat luottamusta asiakkaiden, henkilöstön ja yhteistyökumppaneiden keskuudessa.

10 Oletko kiinnostunut **ISO/IEC 27001 -sertifioinnista?**

Pyydä henkilökohtainen tarjouksesi jo tänään!

Todenna toimiva tietoturvallisuuden hallinta ja toimi kustannustehokkaasti.

Ota yhteyttä

Muut palvelut, joista voit hyötyä

Tarjoamme asiakkaillemme sertifiointipalveluita seuraavien standardien mukaisesti (muun muassa):

- ISO 9001 laadunhallintajärjestelmät
- ISO 14001 ympäristöjärjestelmät
- ISO 45001 työterveyden ja työturvallisuuden hallintajärjestelmät
- ISO 50001 energianhallintajärjestelmät

Asiantuntijamme auttavat sinua mielellään kaikissa sertifioinneissa ja ovat valmiita vastaamaan kaikkiin kysymyksiin.

Hanki DEKRA-sinetti

Maksimaalista laatua ja luotettavuutta osoittava DEKRA-sinetti on erinomainen tunnusmerkki ja markkinointiväline, joka erottaa sinut kilpailijoistasi. Käytä sitä näyttääksesi asiakkaillesi ja liikekumppaneillesi arvosi. Olemme täällä auttaaksemme sinua.